5Rights' comments on the draft Age Appropriate Design Code

May 2019

About 5Rights Foundation

The digital world was imagined as one in which all users would be equal, yet a third of internet users are children.[1] Nearly one billion children are growing up in an environment that systematically fails to recognise their age, and in so doing, fails to uphold the protections, privileges, legal frameworks and rights that together constitute the concept of childhood.

Working closely with children, 5Rights Foundation works towards a digital world that anticipates and supports the presence of children; supporting enforceable regulation and international agreements; developing policy in data protection and child online protection practice; building ethical and child-friendly technical standards and protocols with our network of engineers; and helping businesses re-imagine the design of their digital services.

5Rights Foundation believes that all children need to inhabit a digital environment that anticipates their presence and meets their needs, so they can access it *knowledgeably, creatively, and fearlessly*.

Overview

The digital environment has the power to transform the lives of children, acting as a force for tremendous good and providing them with opportunities that previous generations could only have imagined. But online services can only enhance the lives of children if they are designed with children in mind. The Information Commissioner, Elizabeth Denham CBE, said 'we are not seeking to protect children from the digital world, but to protect them within it'. We support that view and the Commissioner's draft Code, which challenges the status quo in which children's presence is not accounted for by the online services they use.

There is increasing recognition around the world that children require greater recognition in the design and delivery of digital services and digital environments. Many are watching the development of the Code with interest and anticipation. The UK is in a position to lead the world in giving children the specific protection that they merit with regard to their personal data, and to reap the benefits of the innovation that this will inevitably entail.

Since the draft Code was published, we have engaged with a diversity of stakeholders in our broad network, including children themselves, the vast majority of whom have joined us in congratulating the ICO on producing such a thoughtful and thorough draft. We join them now in encouraging the ICO to produce a final version of the Code as soon as is practical, and to lay it before Parliament at the earliest opportunity.

General comments

Intent of the Code

The spirit and purpose of the Code is very clear. It does not seek to constrain the data practices of online services unnecessarily, but it does not allow children's data to be used for diffuse and opaque purposes that have little to no regard for the best interests of the child. It would be helpful for the Commissioner to state at the outset that in assessing compliance, it is how online services have sought to deliver on the ***intent*** of the Code that she will consider.

We recommend: that the Code state that services *must have regard to the intent of the Code, rather than simply the strict letter,* as this will promote good practice and future-proof the Code.

Interconnectedness of the provisions

The sixteen provisions of the Code are all interconnected and inter-reliant, which means that online services must consider them all when interpreting and complying with the Code.

We recommend: that the Code makes clear at the outset that the provisions of the Code must be read in conjunction with each other. Where appropriate, the provisions should be cross-referenced throughout the Code.

Proportionality

The Information Commissioner should set out her criteria for the proportionate application of the Code. Such criteria should include the nature of the data collected or processed, the extent to which the data is collected, processed, or shared, the purpose for which the data is used and the risk that children are exposed to. A clear statement on proportionality, combined with a statement on intent and the existing 'best interests' provision, will allow all parties to assess their own practice and give some assurance to smaller providers who may be concerned about compliance.[2]

We recommend: that the Code spells out the criteria that the Information Commissioner will consider in assessing compliance with the Code.

Age verification

We support the approach taken by the ICO to the age-appropriate application of the Code, which brings an end to the status quo in which online services routinely and wittingly fail to identify children. Recognising the importance of establishing which online users are children and which are adults is part of a larger cultural shift in which users of online services are demanding fairer terms and greater transparency. While age-verification is not currently a norm online, progress can only be made, and further innovation is only likely to follow, when online services are necessitated or incentivised to establish the presence of a child. This is one of the important functions that the Code will serve. [We have made more detailed comments under the relevant provision].

Upholding the rights of children

Children have rights *irrespective* of any harm that may result. We would welcome more reference to the UNCRC to underline that the Code is designed to promote an environment in which a child can *flourish*, not merely be protected from harm.

For instance, 'age-appropriate application' supports a child's right under Article 5 to be treated in accordance with their evolving capacities. 'Nudge techniques' impact on a child's freedom of thought under Article 14 and their right to rest and leisure under Article 31. The provision on 'profiling' supports their right to protection from information or material injurious to their wellbeing

under Article 17(e). 'Transparency' supports a child's right to express themselves in all matters that affect them under Article 12. The Code as a whole defends a child's right to privacy under Article 16.

Additionally, Children have a right to access information from the mass media under Article 17, and the Code should be worded in such a way as to avoid any misconception that news services must move to qualify this right or change their ***news*** content to accommodate children likely to access their site.

We recommend: that the Code is more consistent in referring to the Convention on the Rights of the Child.

Inferred data

The Information Commissioner has made clear that inferred data *is* personal data, most recently in her evidence to the House of Commons Digital, Culture, Media, and Sport Committee in April 2019:

> "Inferred data is personal data… If inferred data is not personal data, it is completely unregulated."[3]

We strongly endorse this important clarification, and the Code could better articulate it throughout.

We recommend: that the Code makes clear overall, or within each provision of the Code, that data inferred or derived from a child's personal data *is* personal data and is therefore subject to the Code.

Purpose and storage limitation

Article 5(1)(b) of the GDPR states that personal data shall be:

> 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'.

This is referred to as the 'purpose limitation' principle and interconnects with the 'data minimisation' principle set out in Article 5(1)(c) (as well as the 'storage limitation' principles under Article 5(1)(e)). These principles are all overarched by the principle of 'accountability', which a service provider needs to implement in order to demonstrate their compliance with the GDPR. Therefore, what service providers do with children's data once it is collected requires as much scrutiny and limitation as whether the data is collected in the first place.

We recommend: that the Code places more emphasis on purpose limitation throughout and, given the importance of this principle, we urge the Commissioner to add an additional provision relating to purpose limitation, or amend the current 'data minimisation' provision to give purpose limitation equal prominence.

'Core service'

We are concerned that more clarity is needed as to what can be considered a core service. For example, many social networks rely on advertising for their revenue, so one such service might describe 'advertising' as its core service rather than 'social network'. Would this mean that serving users with adverts could meet the 'core service' test?

The Code should clarify that 'core service' is limited to the purpose for which a child could reasonably be expected to have accessed the service. It may also be relevant to cross reference the concept of core service with the over-all intent of the Code (see above).

We recommend: that the Code provides a definition of core service that incorporates the principle of purpose limitation and the doctrine of 'reasonable expectations'.

'Compelling reason'

We fully support the acknowledgement that the use of a child's data is often in their best interests. The term 'compelling reason', particularly in relation to the provisions on default settings, data sharing, geolocation, and profiling, is helpful in allowing for reasonable deviation from the Code where it is necessary and in the best interests of the child.

The Code could usefully clarify that what constitutes a 'compelling reason' should be from the point of view of the child. The Code could also provide examples of compelling reasons in different contexts and should outline the criteria by which it will be judged.

We recommend: that the Code clarify that 'compelling' relates first and foremost to the best interests of the child and to the strength of the evidence presented.

Screen-centricity

The Code references non-screen-based services and we welcome the ground-breaking provision relating to connected devices. However, future technology will be increasingly embedded and 'environmental', rather than simply screen-based. The Code should make clear that the nature of the user interface or interaction pattern is not an excuse for failing to comply with its provisions.

We recommend: that the Code include additional, non-screen-based examples in the 'transparency', 'nudge techniques', 'default settings', and 'online tools' sections, among others, to underline the fact that the Code's provisions apply to interactions that may not be screen-based.

Online gaming

There is an absence of examples and language relevant to online games. Online games have tended to be under-associated with data processing, despite the collection of significant and diverse amounts of data from voice recordings and video footage, to user messaging and spending habits.[4] As the Secretary of State, Jeremy Wright, said in evidence to the DCMS Committee in May 2019:

> 'There is no reason in my mind why a games maker should be any more immune from the rules around data protection than any other company or entity would be… If you are misusing data and you find yourself on the wrong side of our data protection rules, you should expect to be subject to the ICO's jurisdiction.'[5]

We recommend: that the Code offers further guidance and examples to help providers of online games to fully understand their obligations under the Code.

Vulnerable groups of children

There is a growing body of evidence that children with special educational needs or disabilities, children in care, young carers, and children with mental health issues face specific challenges online.[6]

We recommend: that the Code explicitly requires online services to properly consider the additional vulnerabilities and needs that such children may have in their Data Impact Assessments and take steps to meet those needs.

Innovation
Innovation and child online protection are not mutually exclusive, and many of those with whom we have engaged see the Code as an exciting opportunity for both innovation and a more diverse digital environment. Increasingly the approach a company takes to privacy and data ethics is seen as a competitive differentiator,[7] and a means of building trust and long-term engagement as children progress in their digital existence. Specifically, we would welcome the Commissioner providing an environment in which online services feel supported to innovate on behalf of children that is in line with their rights to participation (Article 6), right to education (Art 28), and right to development (Article 29), among others.

We recommend: that the Information Commissioner makes a clear statement that whilst all online services must put a child's data protection at the centre of their concern, that innovation and child protection is a false binary and she welcomes the innovation that the Code will bring in its wake.

'Services covered by this Code'

We welcome the Commissioner's statement that the Code 'applies to services that aren't specifically aimed or targeted at children, but are nonetheless likely to be used by under-18s.'

However, greater clarity on the criteria for 'likely to be accessed by children' is necessary. Criteria should include at a minimum: the number and/or proportion of children accessing a service; the nature of a service; if measures are in place to prevent children from accessing the service;[1] and if there are external indicators that children are using the service (e.g. market research or academic research indicating that children routinely use similar online services).

We recommend:

- The Code should set out the criteria by which a service will be judged as "likely to be accessed" by children, including what steps a service might take in their Data Protection Impact Assessments to establish if they meet these criteria. Examples of the kinds of services that lie close to the threshold would also be useful.

Comments on the summary provisions

1. Best interests of the child: The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.

We welcome the inclusion of the 'best interests' test in this Code. This keeps the focus on the needs of the child in the design of service, sets an appropriately high bar for the processing of children's data, and enables services to make proportionate and nuanced decisions about how to comply with the Code.

[1] Ofcom's Broadcasting Code may be useful here in its definition of content 'likely to be accessed by children'. It refers to factors such as 'the nature of the content' and 'the nature of access to the content e.g. ***whether there are measures in place that are intended to prevent children from viewing and/or listening to the content'*** (our emphasis).

2. Age-appropriate application: Consider the age range of your audience and the needs of children of different ages. Apply the standards in this Code to all users, unless you have robust age-verification mechanisms to distinguish adults from children.

The Code is right to recognise that in order to provide children with specific protection for their data, online services must first establish which of their users are children or provide such protection for all users. We welcome the ICO's decision not to stipulate the specific mechanism for age verification or authentication, but instead to require simply that it is done in an effective way, and that data collected for age verification purposes must not then be used for any other purpose.

2.1 Proportionality

This provision would benefit from a statement about how the ICO will interpret their requirement to take 'fair, proportionate and timely regulatory action'.

We support an approach that requires online services to implement demonstrably robust age verification mechanisms if one or more of the following applies to their service: a) it has a large number and/or proportion of child users, b) it poses a particular risk to children, c) it processes a significant amount of personal data, d) it processes particularly sensitive personal data, e) it makes sensitive or impactful judgments on the basis of children's data, or f) it uses children's data to target them with advertising. This should be clearly set in a context of 'best interest' so that where it is demonstrably not in the best interests of a child to age verify (e.g. safeguarding, offering educational opportunities, or access to health services) that it is clear to an online service that they will not be found in breach of the Code.

2.2 Self-declared age

We welcome the Code's move to address the failed system of self-declared age. In the UK, three out of every five children have a social media account by the age of 12, despite a minimum age limit of 13-years-old.[8] In a recent appearance before the House of Commons Digital, Culture, Media and Sport Committee, a representative of Snapchat (which allows users to self-declare their age) conceded that its age verification processes do not work.[9]

However, this is undermined in the section '*Tailor the measures in this code to the age range of your users'*, which allows and encourages services to be tailored to 'the declared age of each user'. This should be redressed.

2.3 'Constructive knowledge'

COPPA has had the effect of disincentivising the implementation of effective age-verification mechanisms by making companies' liable for processing the data of underage users only when they have 'actual knowledge' that they are doing so. Crudely, the worse the mechanism, the less 'actual knowledge' a company has about underage users, so the less liability they have under COPPA.

The Code would be strengthened by clarifying that the Information Commissioner will refer to the 'constructive knowledge' of service providers in assessing compliance with the Code, defined as 'knowledge that one using reasonable care or diligence should have, and therefore that is attributed by law to a given person.'[10] This would incentivise service providers to invest in robust age-verification.

2.4 Preventing services from blocking children

The Code should address the risk (or perceived risk) that some services will choose to respond to the Code by blocking children from accessing them entirely. Our view is that any service inclined to do

that is unlikely to have the best interests of children in mind, and therefore may not be appropriate for children anyway. In any case, however, such a response would clearly undermine the rights of children, so should be avoided. Under COPPA, providers 'may not block children from participating in a website or online service that is directed to children'.[11] The Code could usefully introduce a similar stipulation, making clear that if a service is likely to be accessed by children, children must not be blocked from it (unless there is a compelling reason to do so, taking into account the best interests of the child).

2.5 Technical feasibility

The fact that age verification is not widely applied across the digital ecosphere is a result of commercial interests that favour data collection, a regulatory system that disincentivises oversight (see above 2.3 constructive knowledge) and, as a result of the first two, a lack of investment.

There is also the oft-made argument that it is technically impossible. While age verification is an emerging area, there are already a number of third-party services that are able to establish the age or age range of users in a robust, privacy-friendly and low-friction way. It would take little 'invention' to allow this to happen in a way that is convenient for both users and services.

Additionally, there are many ways of assessing the age or development stage of their users from the way they interact with the services and devices they use. This includes use of language, the way they type, 'pinch' a screen or scroll, even their gait, as well as more 'traditional' data points such as their browsing history and the information they have chosen to share about themselves. These contextual assessments are already widely used by industry for the purposes of commercial profiling,[2] and – subject to the provisions of the Code – could be redirected.

Crucially, progress is only likely to be made in this area when online services are necessitated or incentivised to do so. This is one of the important functions that the Code will serve.

We recommend:

- The Code should make clear that, while wide-spread age verification and assessment is not yet a norm, there are mechanisms available and the Commissioner will expect companies to either implement existing schemes or innovate in order to comply with this provision.
- The Code should clarify that the self-declared age of users is not a sufficient basis on which to tailor a service to age.
- The Code should make clear that the 'constructive knowledge' of online service providers will be taken into account by the Commissioner in assessing compliance with the Code.
- The Commissioner should set out what criteria she will be considering when determining if an online service has acted in a proportionate way in complying with the age-appropriate application provision.
- The Code should make clear that if a service meets the definition of 'likely to be accessed by children', it must not block children from accessing it (unless there is a compelling reason to do so, taking into account the best interests of the child).
- The Commissioner should make a clear statement about the circumstances in which age verification may not be in the best interest of the child, in line with the 'intent' of the Code.

[2] For example, in 2018 various gambling and alcohol advertisers pulled their ad spend from Snapchat citing concerns about Snapchat's ability to prevent these ads being served to minors. Snapchat was quick to refute the concerns, stating that it 'offers amongst the most sophisticated targeting in the industry and by introducing new tools…and incorporating additional signals into our targeting, advertisers have a reliable and flexible way to ensure their ads reach the right audience.' If Snapchat and similar companies are confident that the age verification mechanisms they use to target advertising are effective, we see no reason why they can't be similarly applied to complying with this Code.

3. Transparency: The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.

Transparency is fundamental to fairness and we welcome the careful consideration the Code gives to the needs of children at different stages of development. Given the extent to which so many children's rights are mediated online – free expression, free association, access to information, privacy and the right to have a say in matters that affect them – it is essential that information is presented in ways that allow children to play an active role in balancing the risks and benefits.

3.1 Greater clarity on what services must be transparent about

The intention of the Code is that online services take the minimum amount of data for the shortest amount of time, use it in the least invasive and most purpose-specific ways and share it only when manifestly in a child's best interests. In the small number of cases where this is not happening, it should be clear why they are taking which data, what the potential impact will be on the child, who (specifically) has access to the data, for what purpose, and for how long that data will be held and/or used.

We note that the Code signposts services to Articles 13 and 14 of the GDPR, but believe it should also direct them to the additional transparency provisions set out in Recitals 60 and 61. These are vital and include the following:

- 'The data subject should be informed of the existence of profiling and the consequences of such profiling.'
- 'Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data.'
- 'Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient'
- 'Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information.'

3.2 Fair terms

The provision would be strengthened by including reference to the consumer rights law principles of 'fair terms'. Guidance supporting The Consumer Rights Act (2015) states:[12]

> 'As indicated, openness is not enough on its own, since good faith relates to the content of terms as well as the way they are expressed. Fair dealing has been authoritatively said to require that, in drafting and using contract terms, a trader 'should not, whether deliberately or unconsciously, take advantage' of the consumers' circumstances to their detriment.'

And that:

> 'Businesses need to take particular care in communicating key terms to consumers who may have greater difficulty than others in collecting, processing and acting upon information and thus in exercising choice effectively…for example, young consumers.'

The guidance makes clear that: 'Businesses are not ignorant of how consumers are likely to behave' and must acknowledge the 'inherent biases affecting consumers' behaviour generally' - 'Concerns to fairness are likely to arise where businesses…exploit such biases to their advantage.'

This has implications for the transparency of online services, their use of nudge techniques, the default settings they provide to users, and the content of their terms and policies themselves.

3.3 Children with specific needs in relation to transparency
Consideration should be given to children who may have specific needs in relation to the transparency of published terms. Children who are visually impaired, for instance, or who have special educational needs or disabilities, are equally entitled to a high level of transparency in relation to their data, and we would like to see this further reflected in the Code.

We recommend:

- The Code should clarify what information online services must be transparent about. This need not be an exhaustive list, as ultimately it falls to online services to communicate the information that is important to and impactful on children.
- The Commissioner should include reference to established consumer rights law principles relating to fair and unfair contract terms.
- The Code should outline its expectation that online services consider those children with specific needs in relation to transparency as part of their Data Protection Impact Assessment.

4. Detrimental use of data: Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.

We welcome the safety-by-design requirement implicit in this provision and the ICO's approach of referencing existing codes of practice and formal advice, including the 'precautionary principle' where none exist. Personal data is processed in so many different contexts that no code should seek to address or anticipate every case of detriment that may arise. As providers meet their obligations to undertake a DPIA, they will be in a far better position to consider any detriment that may arise from their processing, having regard to any relevant guidance. The ICO should indicate a broader set of sources that online services could consult in complying with this provision, whilst making clear that an online provider should consider the sources most relevant to the service the child is accessing. Examples could include:

- UK Council for Internet Safety (UKCIS)
- The European Data Protection Board (formerly the Article 29 Working Party)
- ICT Coalition for Children Online
- The Centre for Data Ethics and Innovation (CDEI)
- Alliance to Better Protect Minors Online
- The Office of Fair Trading's Principles for online and app-based games
- Code of Practice on Disinformation (European Commission)
- Internet Watch Foundation's FC Code of Practice
- Code of Practice for Consumer IoT Security
- Consumer rights guidance, including guidance on unfair contract terms
- The UNCRC and forthcoming General Comment on children's rights in relation to the digital environment
- Any codes introduced following the UK Government's Online Harms White Paper.

We recommend:

- The Code should include a greater range of sources of guidance to assist online services with compliance.
- Online services should be asked to consider such guidance and what steps they have taken to meet it as part of their DPIA.

5. Policies and community standards: Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).

We commend the ICO for recognising that processing personal data cannot be 'fair' if online services fail to uphold the rules and policies users have signed up to. In relation to children specifically, published terms allow children, or the adults responsible for them, to decide if the service is age-appropriate and to anticipate any risks it might pose.

We note that this provision brings the Code in line with the Government's Online Harms white paper, which sets out that:

> 'Relevant terms and conditions will be required to be sufficiently clear and accessible, including to children and other vulnerable users. The regulator will assess how effectively these terms are enforced as part of any regulatory action.'[13]

5.1 Fair terms

The Code should align itself with established consumer rights law principles of 'fair terms', 'good faith', and 'fair dealing' (see 3.2). This would serve to mitigate the risk of online services responding to this provision by amending policies and standards to reduce their obligations to users. We note that in its draft guidelines on processing personal data 'necessary for the performance of a contract', the European Data Protection Board states:

> 'Processing of personal data that is based on what is deemed to be an unfair term under the Unfair Contract Terms Directive, will generally not be consistent with the requirement under Article 5(1)(a) GDPR that processing is lawful and fair.'

The Code could also signpost other relevant guidance (see 4.1). For example, the 'Principles for online and app-based games', which specifically relate to children.[14] The principles address the following concerns:

- 'misleading commercial practices, including failing to differentiate clearly between commercial messages and gameplay
- exploiting children's inexperience, vulnerability and credulity, including by aggressive commercial practices
- including direct exhortations to children to buy advertised products or persuade their parents, carers or other adults to buy advertised products for them
- payments taken from account holders without their knowledge, express authorisation or informed consent.'

For absence of doubt, these principles would not be sufficient in-and-of themselves, but applied in conjunction with the other provisions of the Code, they offer helpful further detail to relevant online services.

We recommend:

- In addition to requiring services to uphold their own published rules, the Code should require services to meet fair terms principles under consumer rights law.
- The ICO should consider inserting an appendix, signposting principles of fair, child-friendly terms from other sectors and bodies (whilst making clear they are additional to the requirements of the Code).

6. Default settings: Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).

Default settings are the starting point for children when they first access an online service and are the gateway to giving children the specific protections they are entitled to under the GDPR and this Code.

6.1 Using default settings as a nudge technique

We welcome that the Code makes clear that high privacy default settings must not be used to block or restrict the access of children to services that do not rely on lower privacy settings, and would welcome a statement about intent (see general comments) to prevent an online service using its default settings to get children to behave in ways that are clearly not in their best interests.

6.2 Appropriateness of settings made available to children

The Code is right to say that currently 'many children never change their privacy settings from the default position'. However, it is important to be mindful that most online services have favoured data collection and default settings have been deliberately onerous to change as a result.[15] The Norwegian Consumer Council report *Deceived by Design* states that 'default settings are often sticky' because 'having users opt in to things such as personalised advertising could affect a company's bottom line.'[16]

The Code should also make clear that some settings or options are ***never*** appropriate for children. For example, in an online game or a social network that has both adult and child users, it is not appropriate to allow older users to identify and view the profile of child users and to contact them unsolicited.

We recommend:

- The Code should make clear that default settings must not be used as a nudge to encourage children to make decisions that are not in their best interests, in line with the intent of the Code.
- The Code should clarify that some settings or features are never appropriate for children.
- The Code must explicitly state that default settings that are designed to encourage, or have the effect of encouraging, children towards adopting lower privacy settings will be deemed non-compliant.

7. Data minimisation: Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.

This provision flows directly from Article 5(1)(c) of the GDPR and is a vital protective measure for children.

7.1 'Actively and knowingly engaged'

We endorse the addition of 'actively and knowingly engaged', given the rise in passive collection of data, as well as the widespread practice of online services processing children's data even when they

have navigated away, logged off, or closed a service or app. Clear guidance on how the Commissioner will interpret 'actively and knowingly engaged' would be useful.

7.2 'Processing' not just 'collecting'
Article 5(1)(c) of the GDPR relates to the processing of personal data – as defined under Article 4(2) of the GDPR – and not simply the *collection* of personal data. Despite this, data minimisation is defined in this section as '*collecting* the minimum amount of personal data…', and the rest of the text reflects this narrower understanding. The final draft should include processing as a matter of course.

For example, on page 49 the Code states: 'It is not acceptable to continue to track [a child's] location after they have closed the map or reached their destination'. Instead, the Code should say: 'It is not acceptable to track or further store or process a child's location after they have closed the map or reached their destination'.

7.3 Purpose limitation and storage limitation
These two principles are fundamental to the Code's effectiveness and should be included on an equal basis in this provision (see general notes).

7.4 Bundled permissions
In the current draft, the Code specifically requires online services to refrain from bundling permissions for enhancements, with processing required for the core service. However, this is too narrow.

For example, if an online streaming service requires additional processing to make personalised recommendations to its users, permissions for that processing should not be bundled in with permissions to 'share your data with third parties' or 'show you ads from companies that might interest you'.

The Code should explicitly prevent online services from bundling permissions *in general,* unless there is a compelling reason to do so (having regard for the best interests of the child).

We recommend:

- The Code should clarify how the Commissioner will interpret 'actively and knowingly engaged'.
- The 'data minimisation' provision should be amended to give equal prominence to 'purpose limitation', and emphasise the requirement for 'storage limitation'.
- This section of the Code should be amended to make clear that data minimisation applies to all forms of processing, not just collecting.
- The Code should explicitly prohibit the bundling of permissions unless there is a reason to do so (having regard for the best interests of the child).
- The concept of core service should be clarified to mean the service that a child could reasonably be expected to have understood as the core service, limited to the purpose for which they are accessing it.

8. Data sharing: Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.

The sharing of children's data for purposes that are clear and beneficial should be welcomed, but we fully support the Code in shifting the status quo from one in which children's data is available to anyone and everyone, to one in which children's data is offered a high level of protection.

8.1 Inferred data
Please see comments on this in the general comments section above.

8.2 Transparency
The sharing of data by and between online services is notoriously opaque. In 2017, GPEN found that 51% of websites fail to mention that they share data at all.[17] Which? found that 'consumers tend to operate with an incomplete picture of data sharing and third parties, which means that most are surprised to learn about the extent of the data sharing ecosystem.'[18] The Horizon Digital Economy Research Institute's work with children also found that many were not aware that their data was collected and shared. Where they were aware, they disagreed with it and felt disempowered.[19]

The Code can tackle this lack of transparency in sharing, either in this section or under the transparency provision. In either case, it should be the norm not to share their data, and when it is shared, online services must be required to clearly alert child users, as well as provide clear and prominent details about who specifically their data has been shared with and for what purpose. We note that the European Data Protection's guidance on transparency states that:

> 'In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.'[20]

8.3 Sharing required to provide a service
We are very concerned that the text in this section creates a contradiction with the summary provision itself. Specifically, the Code states:

> 'You should not share personal data if you can reasonably foresee that doing so will result in third parties using children's personal data in ways that have been shown to be detrimental to their wellbeing.'

The summary provision says 'do not disclose' children's data unless there is a 'compelling reason' to do so, which is a higher and more appropriate bar. Children have a right to privacy independent of the potential for harm (see general comments).

If the provision is to work, the starting point must be that a child's data should not be shared unless it is in their best interest. This principle should apply to the sharing of children's data with each individual third party. Being able to justify the sharing of data with one third party does not entitle a service to share data with all third parties (see 7.4).

As an additional safeguard, the Code should also stipulate that a child must not be asked to share data in order to access a service or feature that does not require the sharing of data (see 7.4 and general comment core service). Where a service or feature *does* require the sharing of data, it must only be shared with those parties with whom it is necessary to share it. If a service relies on the sharing of data with *one* third party, that does not mean data can be shared with *another or several* third parties.

The purpose of the Code is to protect children's data, even if that protection conflicts with the commercial interests of the companies whose services they are using. Businesses in all sectors are required to consider the safety and wellbeing of their customers, especially children. As businesses

and whole sectors move online, so too must the protections that they offer to children. As noted in our general comments, this has the potential to create a new market of products and services that prioritise children, leading to a more innovative and competitive environment.

We recommend:

- The Code must make clear that it is only permissible to share a child's data with third parties to the extent that it is necessary to do so in order to provide the service the child is actively and knowingly engaged with, and for the purpose that they might reasonably be expected to have intended.
- Inferred data must be considered as personal data for the purposes of this provision and the Code in general.
- The Code should require online services to be completely transparent about who specifically they are sharing children's data with and why and give convenient opportunities for a child to opt out.
- The Code should stress that sharing must be demonstrably in the best interests of the child.

9. Geolocation: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to off at the end of each session.

We applaud the ICO's recognition in this section that the Code is designed to uphold all the *rights* of children. It states:

> 'It may potentially fail to respect the child's rights under the UNCRC to privacy, freedom of association, and freedom from economic exploitation, irrespective of threats to their physical safety.'

There are many benefits to the processing of children's geolocation data, and many purposes for that processing that clearly serve the best interests of the child. However, geolocation data is also processed for a range of purposes that aren't in the best interests of the child or are deliberately obscured from them. The Code is an invitation to industry to offer geolocation services to children in a manner that is transparent and truly offers them the benefits of the technology, whilst refraining from using their geolocation data in ways or for purposes that are clearly not in their best interests.

9.1 All geolocation tracking should default to off at the end of a session

We welcome the specific requirement that settings which make a child's location visible to other users revert to off when children either navigate away, log off, or are not actively and knowingly engaged with that service or feature. However, the Code should also state that geolocation tracking, even when not visible to other users, should default to off when a child navigates away or is not actively and knowingly engaged with that service (unless there is a compelling reason to continue tracking, taking account of the best interests of the child).

This is consistent with the principles of data minimisation and purpose limitation.

9.2 Different ways of collecting geolocation data

From the perspective of a child, *how* an online service collects their geolocation data is irrelevant, therefore it should not be possible do so without their active and knowing participation. As currently drafted, the Code does not capture the full range of ways that online services are able to collect geolocation data.

For example, many digital cameras record where a photograph is taken and stores that location in the EXIF metadata of the photograph. When a photograph is uploaded to an online service, such as an email provider or social network, that metadata may be stored by the service irrespective of whether a child's settings allow the service to collect geolocation data directly. Some services might 'delete' or 'hide' EXIF metadata from other *users*, but that is not to say that they do not retain it themselves or make it available to other services.

This is just one example among many of how a service might collect a child's location data 'indirectly', even if the child's settings do not allow the service to collect it 'directly'. For example, Facebook's policy states:

> 'When Location Services and Location History are turned off, we may still understand your location using things such as check-ins, events and information about your Internet connection.'[21]

The Code should state that an online service must not collect or process a child's geolocation data *irrespective of where it has come from*, unless the processing is service critical (subject to the 'reasonable expectation' of the child), and that a child is knowingly and actively engaged. In every case the child must be aware of the geolocation data collection and explicitly consent to (and be reasonably expected to understand the implications of) this processing through that specific service.

9.3 Data minimisation/purpose limitation/storage limitation

No more location data should be taken or further processed than is necessary (e.g. if a general location is adequate, then a more precise one must not be collected), the data should not be stored for any longer than is necessary, and inferences must not be drawn from the data unless it is necessary for the functioning of the service (defined earlier in the context of purpose limitation and 'reasonable expectations'). In all cases, it must be necessary to demonstrate a compelling reason to process a child's geolocation data, having regard to the best interest of the child.

In sum, the onus should be on the online service, not the child, to ensure that geolocation data is not collected or further processed or made available either when it is unnecessary to do so or when the child is likely to be unaware that it is being collected. Geolocation data can make a child vulnerable by making their real time location available or easily hackable, but can also provide support if they are lost or in some way require help. Whilst these two scenarios require balanced consideration and thoughtful application, they should not be confused with the routine use of geolocation for commercial profiling. We fully support uses of geolocation that are in the best interests of the child.

We recommend:

- If a child has not given an online service permission to process their geolocation data, the Code should prevent that online service from collecting that child's geolocation data from elsewhere.
- The Code should clarify that the processing of children's geolocation data is subject to the other provisions, and particularly to the principles of data minimisation and purpose/storage limitation.
- The Code should clarify that geolocation tracking should default to off once the child navigates away, unless there is a compelling reason to do otherwise, having regard to the best interests of the child.
- In fulfilling the *intent* of the Code (see general comments) an online service must ensure that a child's default geolocation settings are in the best interests of that child, and do not nudge them to activate geolocation services beyond the purpose they intend.

10. Parental controls: If you provide parental controls, give the child age-appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.

This provision strikes an excellent balance between the rights of children and the responsibility of parents or carers. The provision makes clear that the purpose of parental monitoring services should be to protect and promote the rights of children, not undermine them. Clearly indicating to children that they are being monitored, having regard to their best interests and the stage of their development, is an extremely welcome development.

We note that many commercial services allow or support parental tracking. Parental controls are one feature of child online safety but do not replace the provisions of the Code, parental engagement in a child's online life, nor broader education and discussion about a child's use of technology and safe/unsafe conduct – all of which sit outside the remit of a data protection code.

10.1 Purpose limitation

Parental monitoring and control services often collect extensive and sensitive data on children, which may make children vulnerable to third parties. At a minimum the Code should make clear that data processed for these purposes must not be used for any other purpose. Online services should also be required to demonstrate that they have sufficient security measures in place to prevent parental controls being hacked, as required by Article 32 of the GDPR.

Wherever possible, parental control services should not collect any personal data and instead allow data to flow only between the device of the child and that of the parent (or at least allow for the data to be encrypted).

10.2 Parental controls or permissions are not a substitute for applying the provisions in this Code

The Code should make clear that providing parental controls does not in any way lessen online services' obligation to give children specific protection in relation to their data.

We recommend:

- The Code should make clear that data processed for providing a parental monitoring service or feature must not be used by online services for any other purpose.
- The Code should state that providing parental controls must not be used to allow an online service to fail to comply with the provisions of this Code.

11. Profiling: Switch options which use profiling off by default (unless you can demonstrate a compelling reason for profiling, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).

We agree that profiling should be default off wherever it is possible and appropriate to provide children with a choice, but the Code should also be clear that ***the profiling of children must be limited in general***. This is consistent with Recital 71 of the GDPR and recognises that whilst profiling and personalisation serve a range of purposes, many of them benign or useful, 'it can also lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose'[22] – as well as their right to be treated equally.

This provision should be linked to and indivisible from the data minimisation and purpose limitation principles. That is, services must only collect (or infer) the minimum amount of data necessary to build a profile, where 'necessary' relates to the specific purposes for which the profiling is required.

11.1 Presumption against profiling children

Given the requirements around data minimisation and purpose limitation, the current concentration on default settings alone is inadequate. The Code should state that a child must not be profiled unless:

a) Profiling is essential to the service or feature the child is using
b) Appropriate measures are in place to protect the child from any harmful effects, and
c) It is in a child's best interests.

The Code rightly identifies that profiling can be used for a wide range of purposes, some of which are legitimate and beneficial. What the Code must rule out is the practice of profiling children in limitless and unnecessary detail, for limitless and unnecessary purposes, with no regard for their best interests. If profiling meets the criteria we set out above, it should be allowed only *to the extent and for the purposes that it is necessary.*

If services wish to give children access to services or features that *do not* rely on profiling, but which may be enhanced or improved by profiling, they must first consider whether they have appropriate measures in place to protect the child from any harmful effects. If they cannot demonstrate this, options to activate such services or features must not be made available to children. If they can demonstrate that appropriate measures are in place, these services and features can be made available to children but must be switched off by default and must still comply with the Code's requirements on bundling permissions, data sharing, and data minimisation/purpose limitation.

11.2 Do not profile children to target them with advertising or marketing

The evidence here is unequivocal. Children are less able than adults to identify paid-for content, whether in the form of native advertising, promoted search results, campaign material, or otherwise.[23] Behavioural advertising has a significant impact on children's perceptions and behaviour, exposing their developmental vulnerabilities and threatening both their freedom of thought under Article 14 of the UNCRC and their right to form and preserve their identity under Article 8.[24] Children are more vulnerable and susceptible to 'pressure to purchase', either through prompts to make in-app purchases or games based on 'pay to win' features.[25] As the European Data Protection Board sets out, 'because children represent a more vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes.'[26] Moreover, digital advertising has been found to be 'highly opaque', 'murky', and even 'fraudulent', as stated in evidence to the House of Lords Communications Committee last year.[27]

The Code should make clear that online services must not profile children for the purpose of targeting them with advertising or marketing.

We recommend:

- The Code should prevent online services from profiling children unless there is a compelling reason to do so, having regard to the best interests of the child.
- Where profiling is deemed to be in the best interest of the child, the Code should make clear that its intention is to prevent online services from profiling children either in more detail than is necessary to provide them with the service or feature they are actively and knowingly engaged with, or for purposes that are not necessary to provide that service or feature.

12. Nudge techniques: Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off their privacy protections, or extend their use.

This is a ground-breaking provision, and as far as we are aware, the first time anywhere in the world regulation has sought to address the manipulation of online users through nudge techniques and persuasive design. We are particularly pleased that the ICO has recognised, and moved to prohibit, the widespread practice of online services using nudge techniques to 'lead children to lie about their age' (p.69 in the current draft).

12.1 'Sludge' techniques

In addition to highlighting 'nudge techniques', the Code should highlight the use of 'sludge techniques. While nudge techniques push users towards certain behaviours that are in the interests of an online service, sludge techniques deliberately act as a barrier to users making certain decisions in their own interests. For instance, the Norwegian Consumer Council noted in its research on Facebook's facial recognition services that 'choosing the most privacy friendly option requires four more clicks than the least privacy friendly option'. As the Council point out 'if the aim is to lead users in a certain direction, making the process toward the alternative a long and arduous process can be an effective *dark pattern*.'[28]

12.2 Intention and impact of the nudge rather than the nudge itself

It is important to avoid the misconception that the Code seeks to prohibit the use of any particular design features by online services. Whilst some design features may be judged inappropriate for children in every circumstance (loot boxes being one possible example), the majority of features that can be deployed negatively can also be deployed positively – or neutrally should a service wish to make them so. For example, a pop-up or push notification reminding a child to take a break would not fall foul of the Code in the way that a pop-up or push notification might if it encouraged a child to make an in-app purchase. Equally, a 'like' button could be a simple, private message between two friends, but it could also be used as a public indicator of popularity, driving engagement and maximising data collection. Clarifying that it is the intent and impact of the 'nudge technique' that the Commissioner will consider, rather than the nudge technique itself, is crucial.[3]

12.3 Autoplay

Autoplay features on video-streaming services like Netflix and YouTube, as well as social networks like Instagram, are commonplace. While they are undoubtedly convenient for the user, they are also capable of 'depriving users of a choice about whether or not they want to keep watching'.[29] Irrespective of debates regarding the impact of 'excessive' screen-time, children should be in control of their time, and service features that undermine that control should therefore be ruled out by the Code. Autoplay should be off by default for all child users.

12.4 Nudge (and sludge) techniques in online gaming

Given the nature of online games, many if not most of their features could be categorised as nudge techniques to one extent or another. The Code should provide more clarity for providers of online games, setting out its expectation that techniques used to a) encourage extended use or punish inactivity, b) place financial pressure on children, or c) provide more personal data may fall foul of the Code unless there is a compelling reason for them, taking into account the best interests of the child.

We recommend:

[3] Not least given the headlines that greeted the draft Code's publication, including 'Facebook and Instagram may have to remove "Like" buttons to protect UK children'.

- The Code should clarify that it is the intent and impact of the nudge technique that is important, rather than the nudge technique itself.
- The Commissioner should set out more detailed expectations around the use of nudge techniques in online gaming. In particular, all games played by children must provide them with opportunities to disengage without suffering significant disadvantage in the context of the game.
- Exhortations to make purchases should also be prohibited in relation to children.
- Auto-play must be off by default, and when switched on, revert to off when a child navigates away.

13. Connected toys and devices: If you provide a connected toy or device ensure you include effective tools to enable compliance with this Code.

It is essential that regulation seeks to protect children in all connected environments just as it must protect them when using more traditional, screen-based technologies.

We note that the Government recently announced a consultation on proposals to ensure that connected devices are properly secure, and we welcome the acknowledgement of Minister for Digital and Creative Industries Margot James that security must be 'built-in from the design stage and not bolted on as an afterthought'.[30] This is also true of privacy, particularly where children are concerned. There may be a need for the Code to evolve in light of both what comes of these proposals and the emergence of new technologies, but the Code will be a useful (and more immediate) driver of good practice in this area and is much anticipated around the world.

13.1 Clarity on definition of connected devices

The Code should include a definition of connected devices, and a rationale for why certain devices are in scope and others not. Without a definition, some providers may be unsure if the Code applies to them.

13.2 Communicating information

We welcome the Code's stipulation that connected devices find ways to communicate 'just in time' information clearly, and believe this requirement should be extended to the communication of all information, 'just in time' or not. The absence of a screen-based interface should not give rise to a lack of transparency or failure to uphold other provisions in this Code.

13.3 Passive collection of data

We support the Code's effort to restrict the passive collection of data by connected devices, but 'processing' as well as 'collection' must be limited. A device that needs to collect data to function in listening or stand-by mode, must be subject to data minimisation, purpose limitation, and storage limitation principles.

13.4 Security of connected devices

The security of connected devices is vital, given the sensitive and intimate data they often process. Multiple reports in recent years have warned of insufficient security protections of toys and devices used by children. In 2018, for instance, researchers discovered that a location tracking smartwatch, worn by thousands of children, could be hacked 'with ease', allowing anyone to track their movements.[31]

Article 32 of the GDPR requires providers of online services to 'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk' of their data

processing. The Code should make reference to this and make clear that, where children are concerned, the risk is high and the security of devices must be similarly so.

We recommend:

- The Code should provide a clear and robust definition of connected devices.
- The Code should make clear that the lack of a screen-based interface cannot be used as an excuse for a lack of transparency, or to fall short of upholding the other provisions in this Code.
- The Code should provide greater clarity that connected devices must not collect and process children's data 'passively', or when they are not actively and knowingly engaged with the service.
- The Code should provide more detail on its requirements vis a vis the security of connected devices, in line with Article 32 of GDPR.

14. Online tools: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

14.1 Additional tools to support the rights of the child

The Code has a good list of the kind of tools that services ought to provide, but there are a few additions we can suggest, including:

- A 'show me who has seen or accessed my data' tool
- A 'show me the data inferred or derived from my personal data' tool
- A 'show me my "profile"' tool
- A 'show me a simpler version of these terms and conditions' tool
- A 'reset all my settings to default' tool
- A 'show me what geolocation data you have collected on me' tool
- An 'opt out of all advertising and marketing' tool
- An 'only store this data for X period of time' tool

15. Data protection impact assessments: Undertake a DPIA specifically to assess and mitigate risks to children who are likely to access your service, taking into account differing ages, capacities and development needs. Ensure that your DPIA builds in compliance with this code.

This section is comprehensive and helpful. Asking questions that support the autonomy and rights of children in advance and systematically designing them in, is the greatest hope of making a digital world one in which a child can flourish. A comprehensive DPIA is the very best way of implementing data protection by design, and a good way for companies to demonstrate compliance with it. We particularly welcome the proportionate approach set out in 'step 6', which encourages service providers to identify and assess the level of any risks, and to implement protections, including age verification mechanisms, that are commensurate with those risks.

We recommend:

- As recommended elsewhere, the Code should require online services to include in their DPIAs the steps they have taken to cater for children with specific vulnerabilities or needs.
- The section on DPIAs should make reference to the intent of the Code (see general comments) to ensure that services demonstrate they have considered the intent of the Code, rather than simply the strict letter.

16. **Governance and accountability: Ensure you have policies and procedures in place which demonstrate how you comply with data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children. Ensure that your policies, procedures and terms of service demonstrate compliance with the provisions of this Code.**

We support the breadth and intention of this provision, and note that when we or the children we work with talk directly to developers and engineers, the developers and engineers say - almost without exception - "I never thought about it that way". If the Code can institutionalise consideration of children and their needs or vulnerabilities as a norm, it will go a long way towards driving good design and corporate accountability.

Transition period

While different provisions of the Code may require different periods of time to implement, it is important to note that online services should already be complying with many of the Code's requirements as part of their existing obligations under the GDPR. It has also been suggested from experience that however long the transition, online services will only prioritise implementation just before the deadline.

We recommend that the Information Commissioner makes the transition period as short as is practicable. There is an urgency in the Code's provisions and it has already been a considerable time since the passage of the Data Protection Act 2018. Childhood is short and this regulation is long overdue.

---

[1] One in Three: Internet Governance and Children's Rights, S. Livingstone, et al, Unicef, January 2016
[2] Regulatory Action Policy, ICO, 2019
[3] Elizabeth Denham CBE, House of Commons Select Committee on Digital, Culture, Media, and Sport, April 2019
[4] How big data is disrupting the gaming industry, Kevin Rands, CIO, 2018
[5] Rt. Hon. Jeremy Wright MP, oral evidence to the Digital, Culture, Media and Sport Committee, May 2019
[6] E.g. see Vulnerable Children in a Digital World, Adrienne Katz and Dr Aiman El Asam (Internet Matters), 2019
[7] Data Ethics: The New Competitive Advantage, Guy Hasselbalch and Pernille Tranberg, 2016
[8] Safety Net: Cyberbullying's impact on young people's mental health, The Children's Society and Young Minds, 2018
[9] Snapchat's evidence to the Digital, Culture, Media, and Sport Committee's inquiry on Immersive and addictive technologies, March 2019
[10] Black's Law Dictionary, 2014
[11] COPPA FAQ, Question G3, Federal Trade Commission
[12] Unfair contract terms: CMA37, Competition and Markets Authority, 2015
[13] Online Harms White Paper, UK Government, April 2019
[14] The OFT's Principles for online and app-based games, OFT1519, Office of Fair Trading, 2014
[15] During Mark Zuckerberg's appearance before the Senate's Commerce and Judiciary Committee, it was noted that Facebook allows for high privacy settings, but the user "really has to work at it."
[16] Deceived by Design, Norwegian Consumer Council, 2018
[17] 2017 GPEN Sweep Report, Online Educational Services, Information and Privacy Commissioner of Ontario, October 2017
[18] Control, Alt, Delete, Which?, 2018
[19] Horizon Digital Economy Research Institute response to the Information Commissioner, September 2018
[20] Guidelines on transparency under regulation 2016/679, European Data Protection Board, August 2018
[21] Location History, Facebook, 2019

[22] Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679, Article 29 Working Party, October 2017
[23] Children and Parents: Media Use and Attitudes Report, Ofcom, November 2017
[24] Study on the impact of marketing through social media, online games and mobile applications on children's behaviour, European Commission, March 2016
[25] Principles for online and app-based games, Office of Fair Trading
[26] Guidelines on Automated individual decision-making and profiling for the purposes of regulation, Article 29 Working Party, February 2018
[27] Oral and written evidence, UK Advertising in a Digital Age, House of Lords Select Committee on Communications, April 2018
[28] Deceived by Design, Norwegian Consumer Council, 2018
[29] 'Our minds can be hijacked': the tech insiders who fear a smartphone dystopia, the Guardian, October 2017
[30] Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security, DCMS, April 2019
[31] MiSafes' child-tracking smartwatches are 'easy to hack', BBC, November 2018